11/12/2015

BİL 470

KRİPTOGRAFİ VE AĞ GÜVENLİĞİ

ÖDEV 1

ANALİZ :

- Özet fonksiyonlar arasındaki farkları ve güvenlik değerini tartışın.

MD5 - SHA Karşılaştırması [1]

- MD5'in çıktısı 128 bit iken, SHA'nın çıktısı 160 bittir. Yani MD5'te 4 adet 32 bitlik değişken kullanılırken, SHA'da 5 adet 32 bitlik değişken kullanılır.
- Her ikiside 512 bitlik bloklar üzerinde işlem yaparlar.
- SHA'da ekleme (padding) işlemi, MD5'teki ile aynı şekilde yapılır.
- SHA'da da her 512 bitlik blok için 4 adımda işlemler yapılır, fakat bir farkla: MD5'de her adımda önceden tanımlı işlevlerin kullanımı 16 kez tekrarlanırken, bu sayı SHA'da 20 kezdir.
- SHA girdi olarak maksimum 2^{64-1} uzunluğunda veriyi kabul eder. Bunu yanında MD5 için böyle bir kısıtlama yoktur.
- SHA ürettiği 160 bitlik sonuç ile brute-force (bütün olası sonuçların denenmesi ile gerçekleştirilir) ataklara karşı daha dayanıklıdır.

❖ **Genel olarak SHA, MD5 ten daha güvenlidir.**

Diğer Hash Fonksiyonlar

MD5 ve SHA'nın yanında daha birçok MD algoritması tasarlanmıştır. Bunlardan bazıları:
MD2, MD4, Haval, Ripe-MD, Snefru, N-Hash'dır.

- Veri şifreleme için özet fonksiyonların güvenlik seviyesini tartışın.

Özetleme fonksiyonları, mesaj şifrelemede değil, ya veri güvenliğinde verinin farklı olup olmadığını kontrol etmeye yarar ya da verileri sınıflandırmak için kullanılır. Çünkü çok güvenilir değillerdir.

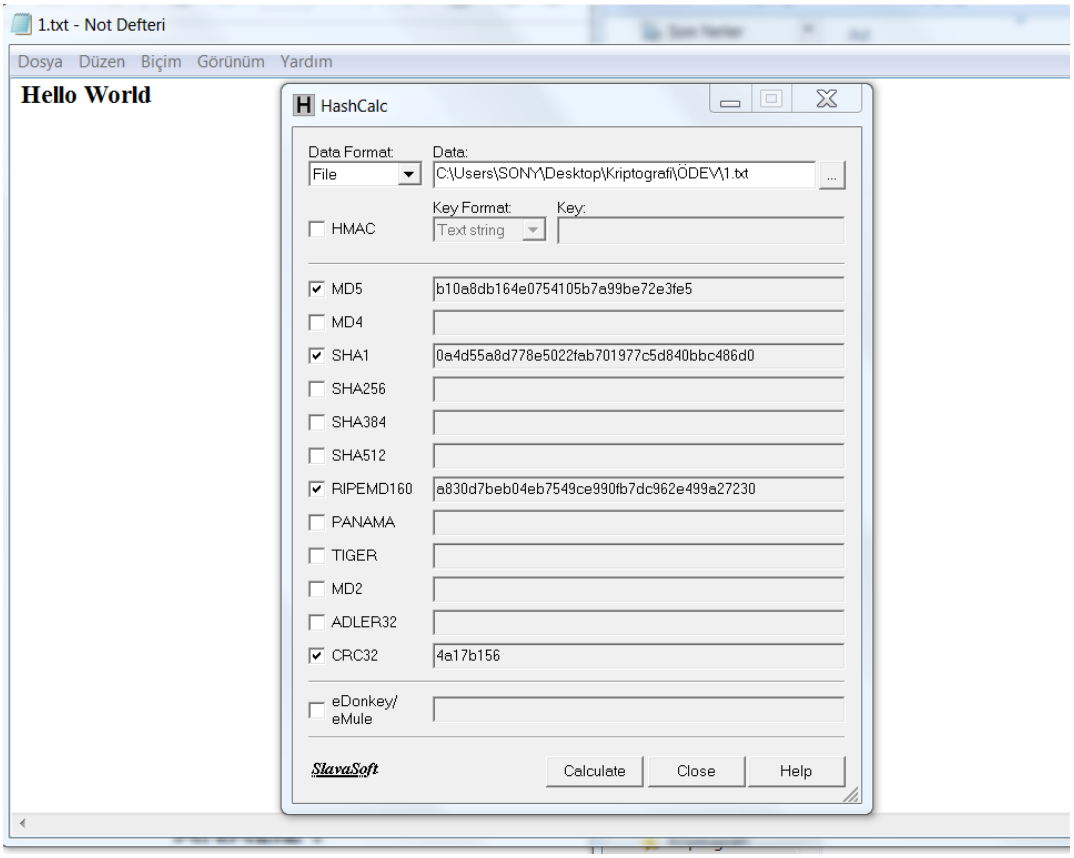
- Aynı özet değere sahip iki farklı doküman olabilir mi ?

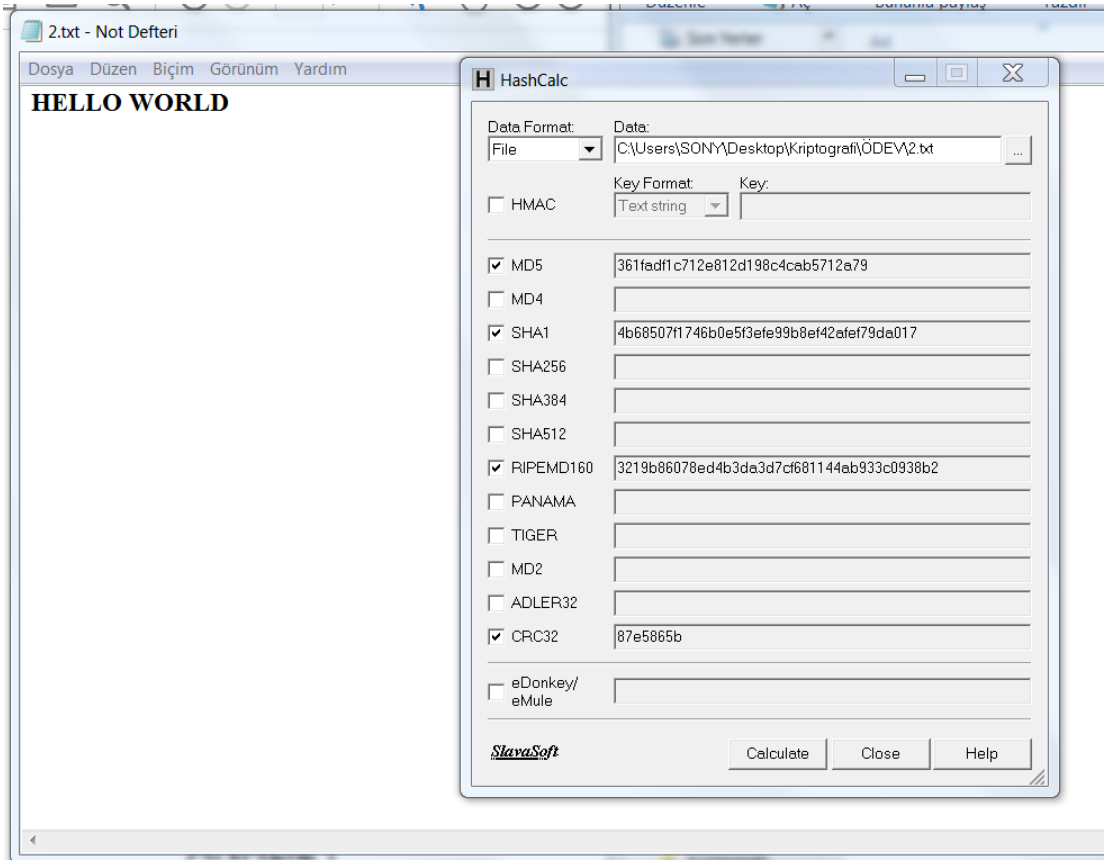
h: {0,1}* ->{0,1}n

Hash fonksiyonu, herhangi bir uzunluktaki açık metni alıp sabit uzunlukta bir çıktı verir. Büyük bir tanım kümesinden sabit görüntü kümesine çoktan-bire eşlemedir.

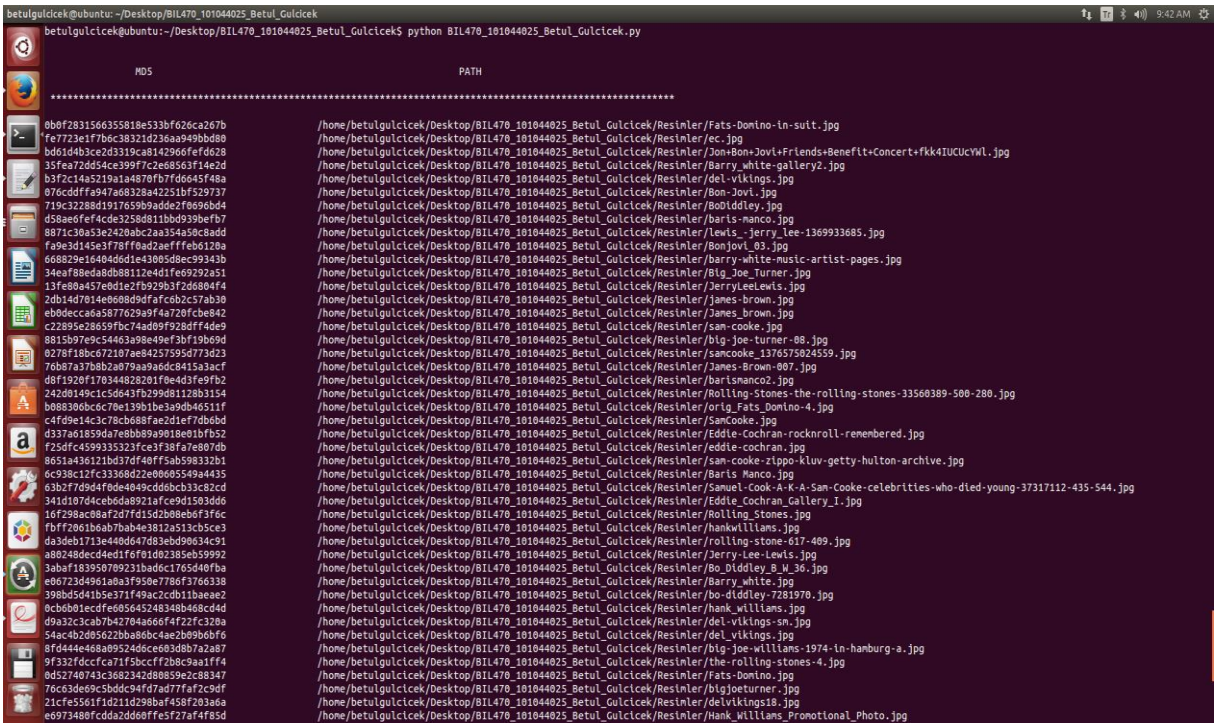
h: Açık Metin -> Özet . Bu nedenle aynı özete sahip metinler bulunabilir.

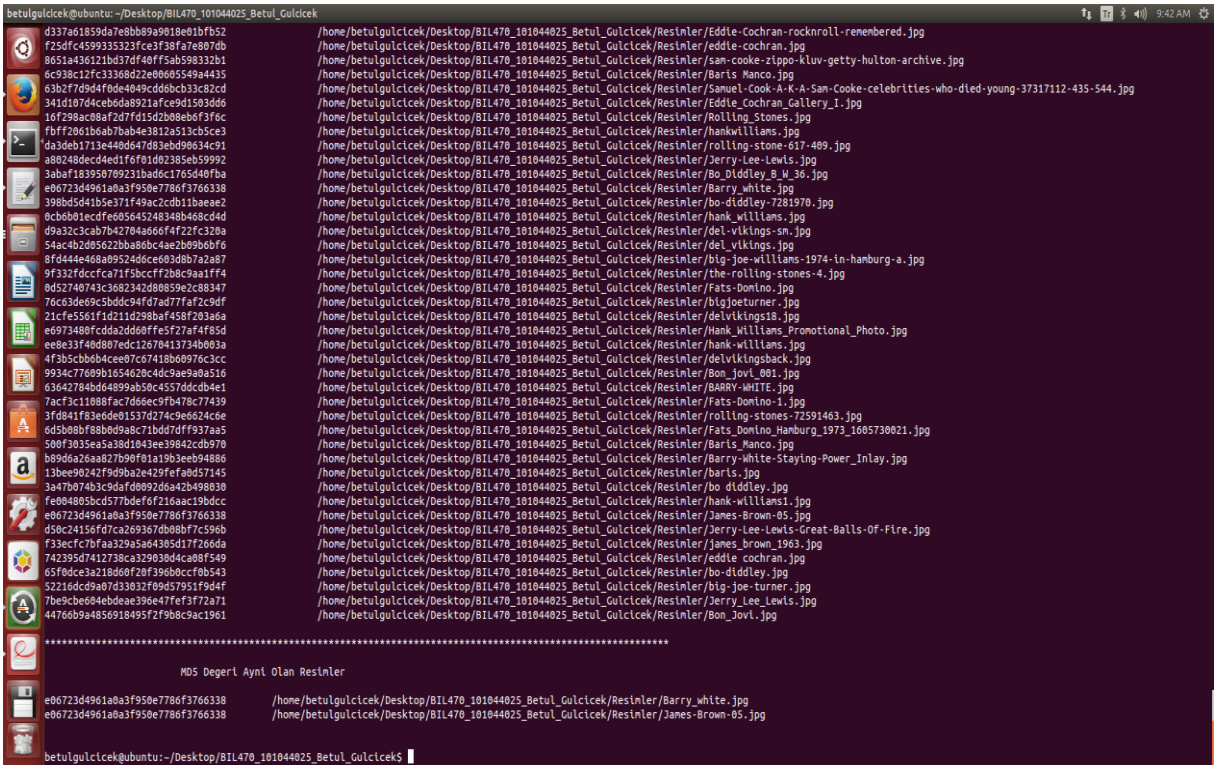
*** Ödevde verilen Hello World ve HELLO WORLD ü denedim ve farklı md5 değerlerine sahip olduğunu gördüm.





Program Çıktım





Kaynak:

[1] *"İleti Özümleme Algoritmaları"*, http://www.belgeler.org/howto/md-algoritmalar.html

BETÜL GÜLÇİÇEK

101044025